Extended Abstract

Hiromitsu Kato <hkato@sdl.hitachi.co.jp>
Systems Development Laboratory, Hitachi, Ltd.
1099 Ohzenji, Asao-ku, Kawasaki 215-0013 JAPAN
TEL: +81-44-959-0244 / FAX: +81-44-959-0851

Security is one of the most critical issues in the field of ubiquitous computing (UbiComp). We have proposed a system architecture to organize distributed objects and to prevent an organized group from experiencing an intentional or accidental denial of services. Several research studies have investigated the use of a computationally rich environment, in which embedded or mobile devices can communicate with each other over a wireless networks. Currently, this kind of ubiquitous environment has the potential to be cooperatively organized for a particular service system. To manifest its potential ability, however, we need an intelligent platform that allows such distributed components to unite to pursue a common objective. In addition to the platform coordinating a system, it would also be responsible for assuring that sufficient security is in place.

One of the results of our UbiComp research was the coining of the term "AYA" to express our basic concept. AYA is an acronym for "context-Aware & Yet Another service". At the same time, AYA is also a Japanese word that means a fabric having a twill-type weave, and twill is derived from the Old English twilic that meant literally "having two threads". Even though a single strand of thread is too simple to express many things, a twilled fabric displays a beautiful pattern woven from thousands of different threads. Similarly, with our AYA concept, we consider that a service system can be built up and emerged by organizing various kinds of component objects, even if each component's behavior is quite simple. Our current goal is to weave pieces of information technologies into a fabric by using AYA, while assuring that the resulting system is secure and privacy concerns are dealt with properly.

To make this flexible system secure, we employed the system model of Secure Tele-operation Protocol (STP), which was originally used as a firewall safeguarding plant control systems, to hold temporary ownership and control of the member devices grouped for a service. In the STP access model, we consider that in the application gateway there is a virtual room, where there exist two kinds of agents. One is a User-Hosting Agent, UHA, which is designed to attend a single user in the manner of the one-on-one defense. The other is an Object-Hosting Agent, OHA, which is designed to protect a control object. The OHA is qualified to manage the operation privileges on the hosting object. The operation privilege can be defined as the current ownership allowing one to get a handle on the registered target object. No one can have access to the object without the corresponding operation privileges given by the OHA. In addition to the strong security, we consider the flexibility that is important to meet the actual operating requirement. Namely, the user is allowed to transfer the operation privileges to another operator with the negotiation protocol regulated in STP.

When we consider the security in UbiComp, we arrange the STP server to form and protect a group. The UHA in the STP server downloads a service logic set from the service provider. Since the service logic contains the design template used to construct a service by logically connecting the necessary functions on the devices, the UHA is able to discover the appropriate objects and to collect the operation privileges of the corresponding device objects that have the necessary functions. At this point, the OHAs are regarded as a cooperative group under the UHA's management. The core program in the service logic controls the behavior of the service. Since the UHA holds the operation privileges during the formation of the service group binding the OHAs, this group cannot be disaggregated even if another request for acquisition of operation privilege comes from another UHA. Additionally, because of the flexibility of STP, the group once formed for a particular service can be restructured with other device objects if the managing UHA changes the membership of the holding target objects. This characteristic improves the stability of the service against the inappropriate access requests, while maintaining the flexibility of the group configuration. This architecture allows us to coordinate the distributed objects to create an ad-hoc service group, while maintaining a sufficient level of security.

For the future work, the peer-to-peer (P2P) architecture holds promise because of its flexibility and survivability. In this case, the functions on a device could be used directly by other devices without having to go through the STP server. The system would utilize some active functions carried on the mobile agents, as well as the fixed functions built in the devices. However, in the P2P world, we must consider more carefully the security issues. Unlike the gateway-centric architecture, distributed device objects must self-protect themselves against various kinds of attacks and disturbances. We postulate that a different kind of approach is necessary.

For further research, smarter sensing of the context would be helpful. In general, the context is defined as the computing context, user context, physical context, and time context. Especially, the location of the user context has been used in many context-aware applications. However, it is still difficult to obtain other useful contexts, such as user's attitude and fickle preferences, and apply them to a useful application. At the same time, we must consider the privacy issues. Context-aware applications are placed in the category of being in a trade-off relationship with regard to privacy, because context sensing without agreement could lead to an invasion of privacy.

So far, we have developed a demo of AYA, which is applied to the town management system (TMS). The TMS is a new concept to enrich the value of a certain commercial areas, such as train station buildings, theaters, museums, and shopping malls, which is powered by UbiComp technology. We developed the "Smart Town Navigation System" (SmartNavi) as a demonstration application. Basically, the SmartNavi looks like a normal car navigation system, which allows a user to obtain a route from their current position to their destination. Since our SmartNavi can reconfigure its service devices, the route information on the PDA can be switched to a larger display around the user based on user's instruction or preference. However, this potential flexibility runs the risk of having a service interruption ensue upon the request of a concurrent device used by another user. To avoid this system deformation during service execution, the embedded STP server handles the competition among the multiple users. Once one user obtains operation privileges for the common display, the others are denied access to the same device with STP's exclusive access control capability until the original user releases the operation privileges.

Our SmartNavi was designed with an awareness of privacy concerns as well. It is necessary to provide some personal information, such as current position and today's schedule, to get more tailor-made route navigation information. However, the user's privacy policy may change according to their situation. Then, we implemented our demo to allow the user to select their own privacy policy, such as a secret mode or a permission mode, as the situation demands.